DATOS IDENTIFICATIVOS DE LA UNIDAD FORMATIVA

UNIDAD FORMATIVA	MONITORIZACIÓN DE LOS ACCESOS AL SISTEMA INFORMÁTICO.	DURACIÓN	90
		Especifica	
Código	UF1353		
Familia profesional	INFORMÁTICA Y COMUNICACIONES		
Área Profesional	Sistemas y Telemáticas		
Certificado de profesionalidad	OPERACIÓN DE SISTEMAS INFORMÁTICOS.	Nivel	2
Módulo formativo	Mantenimiento de la seguridad en sistemas informáticos.	Duración	120
Resto de unidades formativas que completan el módulo	Copia de seguridad y restauración de la información.	Duración	30

Apartado A: **REFERENTE DE COMPETENCIA**

Esta unidad formativa se corresponde con la RP1 y RP2.

Apartado B: **ESPECIFICACIÓN DE LAS CAPACIDADES Y CONTENIDOS**

Capacidades y criterios de evaluación

C1: Identificar los tipos de acceso al sistema informático así como los mecanismos de seguridad del mismo describiendo sus características principales y herramientas asociadas más comunes para garantizar el uso de los recursos del sistema.

CE1.1 Describir los mecanismos del sistema de control de acceso detallando la organización de usuarios y grupos para garantizar la seguridad de la información y funcionalidades soportadas por el equipo informático, según las especificaciones técnicas.

CE1.2 Explicar los procedimientos de los sistemas para establecer permisos y derechos de usuarios, detallando su organización y herramientas administrativas asociadas para organizar políticas de seguridad, según los procedimientos establecidos en el software base.

CE1.3 Clasificar los mecanismos de seguridad comunes en sistemas detallando sus objetivos, características y herramientas asociadas para garantizar la seguridad de la información y funcionalidades soportadas por el equipo informático.

CE1.4 Identificar los mecanismos de protección del sistema contra virus y programas maliciosos para asegurar su actualización.

CE1.5 Identificar los mecanismos de seguridad del sistema para mantener la protección del mismo, según unos procedimientos de operación especificados:

- Identificar los usuarios y grupos definidos en el sistema operando con las herramientas administrativas indicadas en los procedimientos dados.
- Localizar, para cada usuario, los permisos de acceso y las políticas de seguridad asociadas, operando con las herramientas administrativas indicadas en los procedimientos dados.
- Verificar que las aplicaciones antivirus y de protección contra programas maliciosos están actualizadas.
- Comprobar el registro de los usuarios y grupos en el inventario, registrando los cambios detectados.

C2: Interpretar las trazas de monitorización de los accesos y actividad del sistema identificando situaciones anómalas, siguiendo unas especificaciones dadas.

CE2.1 Enumerar los mecanismos del sistema de trazas de acceso y de actividad para su monitorización detallando su ámbito de acción, características principales y herramientas asociadas.

CE2.2 Describir las incidencias producidas en el acceso de usuarios y de actividad del sistema clasificándolas por niveles de seguridad para detectar situaciones anómalas en dichos procesos.

CE2.3 Identificar las herramientas para extraer los ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema para facilitar su consulta y manipulación, de acuerdo a sus especificaciones técnicas.

CE2.4 Interpretar el contenido de ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema para localizar accesos y actividades no deseadas siguiendo el procedimiento indicado por el administrador.

CE2.5 En supuestos prácticos, donde se cuenta con ficheros de traza de conexión de usuarios y ficheros de actividad del sistema, realizar el análisis y la evaluación de los mismos para detectar posibles accesos y actividades no deseadas, según unas especificaciones dadas:

- Identificar las características de un conjunto de registros de usuarios siguiendo las indicaciones del administrador.
- Localizar un registro de un usuario dado y explicar sus características.
- Extraer y registrar las situaciones anómalas relativas a un usuario siguiendo las indicaciones del administrador.
- Documentar las acciones realizadas.

CE2.6 Distinguir las herramientas utilizadas para el diagnóstico y detección de incidencias tanto en aplicación local como remota, para su gestión, solución o escalado de las mismas, según unas especificaciones dadas.

Contenidos

1. Gestión de la seguridad informática.

- – Objetivo de la seguridad.
- – Términos relacionados con la seguridad informática.
- – Procesos de gestión de la seguridad.
  - • Objetivos de la gestión de la seguridad.
  - • Beneficios y dificultades.
  - • Política de seguridad. La Ley Orgánica de Protección de Datos de carácter personal.
  - • Análisis de riesgo.
    - – Identificación de recursos.
    - – Identificación de vulnerabilidades y amenazas: atacante externo e interno.
    - – Medidas de protección.
  - • Plan de seguridad.
- – Interrelación con otros procesos de las tecnologías de la información.
- – Seguridad física y seguridad lógica.

2. Seguridad lógica del sistema.

- – Acceso al sistema y al software de aplicación.
  - • Concepto de usuario, cuenta, grupo de usuario, permisos, lista de control de accesos (ACL).
- – Políticas de seguridad respecto de los usuarios.
  - • Autenticación de usuarios:
    - – Definición y conceptos básicos.
    - – Sistemas de autenticación débiles y fuertes.
    - – Sistemas de autenticación biométricos y otros sistemas.
    - – Acceso local, remote y Single Sing-On.
  - • Herramientas para la gestión de usuarios.
    - – El servicio de directorio: conceptos básicos, protocolos e implementaciones.
    - – Directorios: LDAP, X500, Active Directory.
    - – Herramientas de administración de usuarios y equipos.
    - – Administración básica del servicio de directorio.
- – Confidencialidad y Disponibilidad de la información en el puesto de usuario final.
  - • Sistemas de ficheros y control de acceso a los mismos.
  - • Permisos y derechos sobre los ficheros.
- – Seguridad en el puesto de usuario.
  - • Tipología de software malicioso.
  - • Software de detección de virus y programas maliciosos.
    - – Antivirus, antispyware, firewall, filtros antispam, etc.
  - • Técnicas de recuperación y desinfección de datos afectados.
- – Herramientas de gestión remota de incidencias.

3. Procedimientos de monitorización de los accesos y la actividad del sistema.

- – Objetivos de la monitorización y de la gestión de incidentes de seguridad.
- – Procedimientos de monitorización de trazas.
  - • Identificación y caracterización de aspectos monitorizables o auditables.
  - • Clasificación de eventos e incidencias: de sistema, de aplicación, de seguridad
  - • Mecanismos de monitorización de trazas: logs del sistema, consolas de monitorización de usuarios.
  - • Información de los registros de trazas.
- – Técnicas y herramientas de monitorización.
  - • Técnicas: correlación de logs, de eventos.
  - • Herramientas de monitorización.
    - – Herramientas propias del sistema operativo.
    - – Sistemas basados en equipo (HIDS).
    - – Sistemas basados en red (NIDS).
    - – Sistemas de prevención de intrusiones (IPS).
- – Informes de monitorización.
  - • Recolección de información.
  - • Análisis y correlación de eventos.
  - • Verificación de la intrusión.

- Alarmas y acciones correctivas

– Organismos de gestión de incidentes:
- Nacionales. IRIS-CERT, esCERT.
- Internacionales. CERT, FIRST.

Apartado C: **REQUISITOS Y CONDICIONES**

Deberá cumplir alguno de los requisitos siguientes:

- Estar en posesión del título de Graduado en Educación Secundaria Obligatoria.
- Estar en posesión de algún certificado de profesionalidad de nivel 2.
- Estar en posesión de un certificado de profesionalidad de nivel 1 de la misma familia y área profesional.
- Cumplir el requisito académico de acceso a los ciclos formativos de grado medio o haber superado las correspondientes pruebas de acceso a ciclos de grado medio.
- Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
- Tener, de acuerdo con la normativa que se establezca, los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.

En relación con las exigencias de los formadores o de las formadoras, instalaciones y equipamientos se atenderá las exigencias solicitadas para el propio certificado de profesionalidad.